

CLAIMS

1. A recording and reproducing apparatus,
comprising:

at least one of a recording portion for
recording encrypted data to a recording medium having
first information that is unique thereto and a
reproducing portion for reproducing encrypted data
recorded on the recording medium;

a storing portion for storing second
information uniquely assigned to a valid electronic
apparatus or valid application software; and

a connecting portion for mutually
authenticating a data processing apparatus for at least
encrypting data or decrypting encrypted data with a key
generated in accordance with both the first information
unique to the recording medium and the second
information stored in the storing portion.

2. The recording and reproducing apparatus as
set forth in claim 1,

wherein a part of the second information is
stored in the storing portion,

wherein the other part of the second
information is stored in the data processing apparatus,
and

wherein the part of the second information
stored in the storing portion and the other part of the
second information stored in the data processing

apparatus are combined as the second information.

3. The recording and reproducing apparatus as set forth in claim 1,

wherein the data processing apparatus has a
5 revoke processing portion for performing revocation
with at least the second information stored in the
storing portion and the first information unique to the
recording medium when the second information stored in
the storing portion is not information unique to a
10 valid electronic apparatus or valid application
software, and

wherein the connecting portion is configured
to send the second information stored in the storing
portion to the data processing apparatus.

15 4. The recording and reproducing apparatus as set forth in claim 3,

wherein the second information that is sent
is encrypted.

20 5. The recording and reproducing apparatus as set forth in claim 1, further comprising:

a revoke processing portion for performing
revocation with the second information stored in the
storing portion and the first information unique to the
recording medium when the second information stored in
25 the storing portion is not information unique to a
valid electronic apparatus or valid application
software.

6. A recording and reproducing apparatus,
comprising:

at least one of a recording portion for
recording encrypted data to a recording medium having
first information that is unique thereto and a
reproducing portion for reproducing encrypted data
recorded on the recording medium;

a storing portion for storing second
information uniquely assigned to a valid electronic
apparatus or valid application software;

a connecting portion for mutually
authenticating a data processing apparatus for at least
encrypting data or decrypting encrypted data with a key
generated in accordance with both the first information
unique to the recording medium and the second
information stored in the storing portion; and

a revoke processing portion for performing
revocation with the second information sent from the
data processing apparatus through at least the
connecting portion and stored in the storing portion
and the first information unique to the recording
medium when the second information stored in the
storing portion is not information unique to a valid
electronic apparatus or valid application software.

7. The recording and reproducing apparatus as
set forth in claim 6, further comprising:

decrypting means for decrypting the encrypted

second information.

8. A data processing apparatus, comprising:

a connecting portion for mutually

authenticating a recording and reproducing apparatus

5 for at least recording encrypted data to a recording
medium having second information uniquely assigned to
only a valid electronic apparatus or valid application
software and first information unique thereto or
reproducing encrypted data therefrom; and

10 a processing portion for at least encrypting
data or decrypting encrypted data with a key generated
in accordance with both the first information unique to
the recording medium and sent from the recording and
reproducing apparatus through the connecting portion
15 and the second information unique to the electronic
apparatus or application software.

9. data processing apparatus as set forth in
claim 8,

20 wherein a part of the second information is
stored in the storing portion,

wherein the other part of the second
information is stored in the recording and reproducing
apparatus, and

25 wherein the part of the second information
stored in the storing portion and the other part of the
second information stored in the data processing
apparatus are combined as the second information.

10. The data processing apparatus as set forth in
claim 8,

5 wherein the data processing apparatus has a
revoke processing portion for performing revocation
with both the second information sent from the
recording and reproducing apparatus through the
connecting portion and the first information unique to
the recording medium when the second information is not
10 information unique to a valid electronic apparatus or
valid application software.

11. The data processing apparatus as set forth in
claim 10, further comprising:

15 decrypting means for decrypting the encrypted
second information.

12. The data processing apparatus as set forth in
claim 8,

20 wherein the data processing apparatus is
connected to the recording and reproducing apparatus
that has a revoke processing portion for performing
revocation with both the second information stored in
at least the recording and reproducing apparatus and
the first information unique to the recording medium
when the stored second information is not information
25 unique to a valid electronic apparatus or valid
application software.

13. A data processing apparatus, comprising:

a storing portion for storing second
information uniquely assigned to only a valid
electronic apparatus or valid application software;

5 a connecting portion for mutually
authenticating a recording and reproducing apparatus
for at least recording encrypted data to a recording
medium having first information unique thereto and
reproducing encrypted data recorded on the recording
medium; and

10 a processing portion for at least encrypting
data or decrypting encrypted data with a key generated
in accordance with both the first information unique to
the recording medium and the second information stored
in the storing portion,

15 wherein the second information stored in the
storing portion is sent to the recording and
reproducing apparatus that has a revoke processing
portion for performing revocation when the second
information stored in the storing portion is not
20 information unique to a valid electronic apparatus or
valid application software.

14. The data processing apparatus as set forth in
claim 13,

25 wherein the second information that is sent
is encrypted.

15. A recording, reproducing, and processing
system, comprising:

a recording and reproducing apparatus for
at least recording encrypted data to a recording medium
having first information that is unique thereto or
reproducing encrypted data recorded on the recording
5 medium, the recording and reproducing apparatus having
second information uniquely assigned to a valid
electronic apparatus or valid application software; and

10 a data processing apparatus for at least
encrypting data or decrypting encrypted data with a key
generated in accordance with both the second
information at least stored in the recording and
reproducing apparatus and the first information unique
15 to the recording medium.

16. The recording, reproducing, and processing
system as set forth in claim 15,

20 wherein the data processing apparatus has a
revoke processing portion for performing revocation
with the first information unique to the recording
medium and the second information stored in the data
processing apparatus when the second information stored
therein is not information that is unique to a valid
electronic apparatus or valid application software.

25 17. The recording, reproducing, and processing
system as set forth in claim 15,

wherein the recording and reproducing
apparatus has a revoke processing portion for
performing revocation with the first information unique

to the recording medium and the second information stored in the data processing apparatus when the stored second information is not information that is unique to a valid electronic apparatus or valid application software.

5

18. A recording, reproducing, and processing system, comprising:

10

a recording and reproducing apparatus for storing second information uniquely assigned to only a valid electronic apparatus or valid application software and at least recording encrypted data to a recording medium having first information unique thereto or reproducing encrypted data recorded on the recording medium; and

15

a data processing apparatus for encrypting data or decrypting encrypted data with a key generated in accordance with both the second information stored in the recording and reproducing apparatus and the first information unique to the recording medium,

20

wherein the data processing apparatus is configured to send the second information stored in the storing portion thereof to the recording and reproducing apparatus having a revoke processing portion for performing revocation when the second information stored in the recording and reproducing apparatus is not information unique to a valid electronic apparatus or valid application software.

25

19. A recording and reproducing apparatus,
comprising:

at least one of a recording portion for
recording encrypted data to a recording medium on which
5 first information for revoking an invalid electronic
apparatus, second information that is unique to each
content, third information that can be defined for each
encrypting unit, and identification data that is unique
to each stamper are recorded and a reproducing portion
10 for reproducing encrypted data from the recording
medium;

a storing portion for storing fourth
information uniquely assigned to a valid electronic
apparatus or valid application software,

15 a revoke processing portion for determining
whether or not the stored fourth information is
information unique to a valid electronic apparatus or
valid application software in accordance with the first
information and the fourth information; and

20 a calculating portion for obtaining
intermediate key information unique to each recording
medium in accordance with the first information, the
fourth information, the second information, and the
identification data when the revoke processing portion
has determined that the fourth information is
25 information unique to a valid electronic apparatus or
valid application software.

20. The recording and reproducing apparatus as set forth in claim 19, further comprising:

5 an authenticating portion for mutually authenticating a data processing apparatus for at least encrypting data or decrypting encrypted data with a key generated in accordance with the intermediate key information; and

10 an intermediate key information encrypting portion for encrypting the intermediate key information with a bus key generated when the authentication has been successful and sending the encrypted intermediate key information to the data processing apparatus.

21. A data processing apparatus, comprising:

15 an authenticating portion for authenticating a recording and reproducing apparatus for at least recording and reproducing encrypted data to and from a recording medium on which fourth information uniquely assigned to a valid electronic apparatus or valid application software, first information for revoking an invalid electronic apparatus, second information unique to each content, third information that can be defined for each encrypting unit, and identification data unique to each stamper are recorded;

20 a key information decrypting portion for receiving from the recording and reproducing apparatus intermediate key information unique to each recording medium, the intermediate key information being

generated in accordance with the first information, the fourth information, the second information, and the identification data having encrypted with a bus key generated when the authentication has been successful;

5 an encryption key generating portion for generating an encryption key with the third information received from the recording and reproducing apparatus and the decrypted intermediate key information; and

10 an encrypting and decrypting portion for at least performing encryption with the encryption key or performing decryption with the encryption key.